

(6)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-220684

(43)Date of publication of application : 13.09.1988

(51)Int.Cl.

H04N 7/16
H04H 1/00

(21)Application number : 62-054558

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 10.03.1987

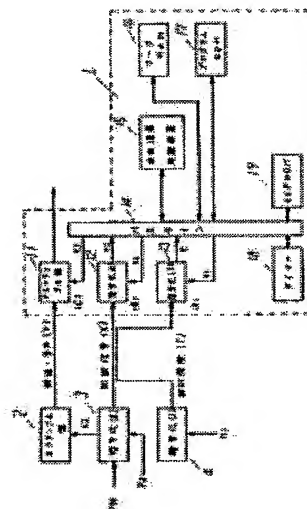
(72)Inventor : HIRASHIMA MASAYOSHI

(54) TERMINAL CONTROL SYSTEM

(57)Abstract:

PURPOSE: To continuously receive only formal terminal of which procedure is finished by previously sending a next key which becomes effective in a fixed term to a tariff prepayment terminal, canceling a former key with the aid of timer output and writing a new key in a decoder.

CONSTITUTION: When a timer 18 automatically generates an off-signal at the end of a month or the beginning of a month and stops sending an cipher key K2 to the decoding part 12, the decoding part 12 can not decode. Therefore a cipher key K3 cannot be obtained and both of an image and a voice cannot be decoded. On the other hand, the ciphered information on a next month pay ment, the key K2 and time information are simultaneously sent with a terminal address to the terminal in which the next month tariff is paid for until a fixed date from a center. Thus after passing the fixed term, the tariff non-payment terminal automatically cannot decode the cipher.



(6)

訂正有り

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭63-220684

⑬ Int. Cl.⁴

識別記号

庁内整理番号

⑭ 公開 昭和63年(1988)9月13日

H 04 N 7/16
H 04 H 1/00

C-8321-5C
F-7608-5K

審査請求 未請求 発明の数 1 (全7頁)

⑮ 発明の名称 端末制御方式

⑯ 特 願 昭62-54558

⑰ 出 願 昭62(1987)3月10日

⑱ 発 明 者 平 嶋 正 芳 大阪府門真市大字門真1006番地 松下電器産業株式会社内

⑲ 出 願 人 松下電器産業株式会社 大阪府門真市大字門真1006番地

⑳ 代 理 人 弁理士 中尾 敏男 外1名

2 ページ

明 細 書

1、発明の名称

端末制御方式

2、特許請求の範囲

(1) 多数の端末器をセンターから制御できる情報伝送システムにおいて、端末器内に、第1の暗号化鍵 K_1 で暗号化された時刻情報を復号化する機能Aと、第2の暗号化鍵 K_2 で暗号化された端末制御信号 X を復号化する機能Bと、第3の暗号化鍵 K_3 で暗号化された情報 Y を復号化する機能Cとを有し、機能Bにより、機能Cの動作を停止或は開始させる事を特徴とする端末制御方式。

(2) 機能Bの復号出力 K_3 をEEPROMにメモリーし、機能A、B、Cを実行させるプログラムを書込んだROMと機能A、B、Cを実行するハードウェアの一部又は全部とこれらを制御する中央演算処理部と上記EEPROMと、上記EEPROMとを同一基盤上に集積化し、密封し、開封しても顕微鏡等により拡大しない限

り上記A、B、Cを実行するハードウェア、

EEPROM及びROMのレイアウト、回路構成が判別できないような集積回路素子を用いてなる特許請求の範囲第1項記載の端末制御方式。

(3) 第1の鍵 K_1 と第2の鍵 K_2 を共通にした事を特徴とする特許請求の範囲第1項又は第2項記載の端末制御方式。

3、発明の詳細な説明

産業上の利用分野

本発明はCATV或は衛星放送等で有料放送を実施する場合の料金不払端末の制御と、料金支払済端末を聴視可に設定することができる端末制御方式に関するものである。

従来の技術

CATV或は衛星放送等に利用されるシステムにおいては、料金未払端末に、強制オフ信号を送って、聴視不可としていた。また、盗聴を防止するために多層鍵による方式も考えられている。

発明が解決しようとする問題点

しかしながら、上記のような多層鍵による方式

特開昭63-220684 (2)

3 ページ

は構成が複雑になる等、以下のような不都合を有していた。

- (1) 強制オフ信号を各端末毎に送る場合、端末が電源オフされていれば、オフにできないので、オフ情報を絶えず送り続けねばならず、端末が多くなると、その端末がアクセスされて、オフされるまでに相当の時間が必要となり、その間不正視聴が可能である。例えば、1フィールドで一端末をアクセスすると、1日24時間で518万4千端末をアクセスできる。仮に全国3千万世帯中1%が毎月不払いとなれば30万世帯をアクセスする必要があり、1時間で21万6千世帯だから約1時間半毎に1回アクセスできる。従って不払いでも平均して約 $\frac{1}{2} \times 90$ 分、即ち45分は不正に見られるので、5分或は10分見る毎にオフレオフ期間を長くすれば、料金未払いでも視聴できる。

- (2) 毎月、月末、月始めに、端末をオンする情報を送る場合、各端末のアドレスをアクセスする為には、加入者3千万で1フィールド毎に一端

末をアクセスすると約6日必要となり、端末が約1週間連続通電される必要がある。端末のACコードがこの間に抜かれているとオン情報は伝わらない。

- (3) タイマーを内蔵し、月末に自動オフする方式ではタイマーの電源がオフになると誤動作する。本発明は上記問題点に鑑み、不正聴取が困難な端末制御方式を提供せんとするものである。

問題点を解決するための手段

本発明は上記目的を達するため、多数の端末器をセンターから制御できる情報伝送システムにおいて、端末器内に、第1の暗号化鍵 K_1 で暗号化された時刻情報を復号化する機能Aと、第2の暗号化鍵 K_2 で暗号化された端末制御信号 X を復号化する機能Bと、第3の暗号化鍵 K_3 で暗号化された情報 Y を復号化する機能Cとを有し、機能Bにより、機能Cの動作を停止或は開始させる構成となっている。

作用

本発明は上記した構成により、料金未払端末鍵

5 ページ

K_2 による復号を停止すると共に、料金前納端末に、次の一定期間有効となる鍵を予め送っておき、タイマー出力で前の鍵をキャンセルし、新しい鍵を復号器へ書き込むことで、正規の手続済端末のみ継続して受信でき、料金支払済期間終了後は、未払端末は受信不能となる。

実施例

本発明の一実施例を第1図に示す。第2図の ϕ_1, ϕ_2 に伝送信号のフォーマットを示す。1パケット中ヘッダー16ビット、メッセージ190ビット、訂正ビット82ビットとすると文字放送のBIST方式が使える。本発明の動作の概要を述べる。端末をアクセスする場合、先ず時刻コード T をDESで暗号化し、第2図に示す ϕ_1 のメッセージの中へ64ビットで入れて送る。暗号化及復号化は共通鍵 K_1 で行えるものとし、各端末とセンター間是一对で、端末の数だけ鍵があるものとする。時刻コードを復号化部13で復号化し、タイマー18を校正する。校正は端末アクセスの都度行うものとする。又、同時に190-64=

6 ページ

126ビットの他のメッセージも送られる。ここで端末アドレスを暗号化せずに入れておいてもよい。タイマー18からオフ情報が出る迄、鍵 K_2 で暗号化されたPNコード、即ち制御信号 X は復号化部12で復号化される。復号化部12の出力の K_3 で、スクランブルされた映像及音声信号を復号(デスクランブル)し、映像、音声を得る。

以下、第1図～第3図と共に更に詳しく述べる。第2図の ϕ_1, ϕ_2 又は ϕ_3 はVBL中の10～17Hに8パケット分重畳されるものとし、各端末への時刻情報は K_1 で暗号化されているので不正視聴のため、処理回路1へ、偽の時刻情報を入力する事はDESを解く事になり実質的に不可能である。

第3図において25は同期再生回路、22は第10～17Hの各Hの水平走査期間に重畳された ϕ_1 の各288ビットのみを抜取る抜取回路、23は抜取回路22の出力をパルスに整形する2値整形回路、24はIC化されたBIST方式の誤り訂正回路で、1フィールド内に8パケット処

特開昭63-220684 (3)

7 ページ

理できるものである。(1フィールド1パケットの処理能力なら、誤り訂正回路24は8LSIにすればよい。)誤り訂正回路24の出力が暗号解読処理回路1'の復号化部12,13へ供給される。暗号解読処理回路1'は第1図の処理回路1から、ビデオメモリ11M、復号制御回路11V、音声再生回路11Sを除いた部分である。尚、復号制御回路11Vはビデオメモリ11Mからの読出しを制御するもので、音声再生回路11SはPCM復調と、PCM復調出力の暗号解読を行なう回路である。

さて、映像信号を第3図に示すDET21で検波して取り出す。仮に衛星放送とすれば、DET21はFM検波回路である。DET21の出力中の例えば、6.73Mの音声キャリアを音声再生回路11Sで復調する。音声はPCMの時、デジタル処理は容易であり、第1図のスクランブル部2で、暗号化されたPN信号K₃で暗号化して送られる。映像は、ランダム反転或はラインバミューティション等K₃を用いて暗号化される。映像

信号はビデオメモリ11Mに記憶される。ビデオメモリ11Mは1フィールド分でも、それ以下の容量のものでも又、アナログでもデジタルでも差支えない。一方、K₃を得るためのK₂は、例えば1カ月(2カ月或は0.5カ月毎)に変化するものとすれば、タイマー18からオフ情報が出ない限り、CPU15とワークRAM16、プログラムROM17の内容による処理によって、K₂が復号化部12へ伝えられており、第3図に示す復号化部12,13へ誤り訂正された各パケットのメッセージが入力され、復号され、CPU15、ワークRAM16、プログラムROM17で判定され、必要な情報K₃等がワークRAM16の一部へメモリされる。さて、タイマー18で、月末又は月始め(毎月1日零時零分)にオフ信号を自動的に発生させ、即ちCPU15、ワークRAM16、プログラムROM17でこれを判定、検出し、バスライン14を介して、復号化部12へ鍵K₂を送るのをやめると、復号化部12では復号できなくなり、K₃が得られず画像、音声共に復

9 ページ

10 ページ

号できなくなる。一方、所定期日迄に翌月の料金を支払った端末には、センターから端末アドレス(非暗号化)と共に、第2図のφ₁の如く暗号化して、翌月分支払済情報と鍵K₂を時刻情報と共に送る。即ち、アドレス30ビットで10億個まで端末判別でき、暗号化された88ビットの料金情報で、何月分か、何円払ったか、どんなジャンル、番組を見たいか等々の情報と鍵K₂が送られる。これらの情報を月末までに受信し、EEPROM19の所定の位置にメモリしている時はタイマー18より、オフ信号が出力されても、CPU15、ワークRAM16、プログラムROM17は、その信号を無視し、次の月のK₂を復号化部12へ与える。このような動作は、全部プログラム処理しても、全部ハードロジックで処理しても、両者混合してもよい。料金情報をEEPROM19へ書込むので、受信機のAC電源がオフになっても、タイマー18がバッテリーバックアップで、そのバッテリーが除去されたとしても、EEPROM19の内容は保持されるので、再び電源を供給す

れば、EEPROM19からK₂を読み出すことができる。

上記の説明では、時刻コードが不正解読されないよう各端末毎に、その端末をアクセスする都度、タイマーを校正したが、時刻コードは全端末共通の鍵K₁(以下前の説明と区別するためK₁'と記す)で暗号化する場合を考える。K₁'は送受システム運用者及び機器製造者が知り得るがK₁'を知って時刻情報を偽造し、第3図の誤り訂正回路24の出力の代りに、暗号解読処理回路1'へ入力しても、料金情報及鍵K₂を別の鍵K₀で暗号化し、K₀を端末毎に別々にすれば、第2図のφ₁,φ₂の形と同一の秘密性が保たれる。この場合、端末アクセス中はφ₅を7H、φ₃は1Hに重畳し、毎分1回φ₄をφ₅の代りに送る。端末非アクセス時は、8H共φ₅を重畳し、毎分1回φ₄をφ₅の代りに送る。この時、受信側は、第4図の如くなる。第4図は主要部を示し、誤り訂正回路24でφ₁~φ₅のメッセージ190ビットを誤り訂正し、バッファメモリ33へメッセージ

特開昭63-220684(4)

11 ページ

190ビットをメモリさせる。バッファメモリ33の内容を中央演算処理装置15と、ワークRAM16、プログラムROM17により判定する。まず制御の8ビットでパケットの種類 ϕ_3 、 ϕ_4 、 ϕ_5 かを判定し、 ϕ_4 の時、最初の64ビットを K_1' で復号する。この64ビット中の時刻コード39ビットをバスライン14を介してタイマー18へ書込む。この時、中央演算処理装置(以下CPUという)15より、I/Oポート(出力ラッチ付)を低レベルとして、バスライン14のデータ、アドレスをタイマー18へ入力可とし、フリップフロップ(以下FFという)32をリセットする。電源オン時、主電源の立ち上りのエッジで、FF32がセットされているので、Qが低レベルになっており、これが、I/Oポート30を介し、CPU15へ伝えられているので、タイマー18へ ϕ_4 の中の時刻コードを1回書込むと、FF32のQが高レベルになって、CPU15の入力ポートが高レベルになる。従って、以降 ϕ_4 は無視する。以降タイマー18から例えば

1時間毎に、信号(59分00秒)をバスライン14を介して取り出し、CPU15で、バッファ33に ϕ_4 のデータがメモリされるのを待つ。タイマー18の誤差は、タイマー18を水晶で構成すれば月差15秒程度となるので、電源オン時に1回、時刻を校正すれば、以降60分毎に、時刻コードを取り込みタイマー18を校正する。送信側で、予め毎時00分の前後1〜2分間、重要情報を送らなければDESの鍵 K_1' を用いて、時刻コードを復号する事にCPU15、ワークRAM16、プログラムROM17を~~専念~~させ得る。それ以外の期間で、DESによる復号を行なうのは端末がアクセスされた時、つまり月1回のみである。従って、送り側でDESにより暗号化した信号を送る時、その後、一定時間、端末にとって重要な信号を送らないか、何回も続けて送るかして受信側でDES復号中に重要信号を検出されすることは無い。また、 ϕ_5 の如く1パケット内に3端末分のデータを送ることもでき、アクセス時間は短かくできる。

13 ページ

尚、このアクセス時間について簡単に説明すると、8パケットの場合、7パケットをアクセスに、1パケットは制御用に使うと、1パケットー端末として、

$$\begin{aligned} 60 \times 60 \times 7 &= 25200 / \text{分} \\ 151.2 \text{ 万} &\text{ 端末 / 時間} \\ 3628.8 \text{ 万} &\text{ / 日} \end{aligned}$$

アドレスを25ビットとし、3200万端末に制限し時刻コードをBCDで現わし、年は8ビット、月は4ビット+1ビット、日は4ビット+2ビット、時は4ビット+2ビット、分は4ビット+3ビット、秒は4ビット+3ビットとすると全部で39ビットとする。1アドレス当り料金情報を27ビットにすると、1パケット190ビット中制御信号8ビットを除く182ビットが $(25+39+27) \times 2$ となり、2端末を1パケットでアクセスでき、1時間当り302.4万/時間即ち、3000万なら10時間でアクセスできる。アドレス以外の各66ビットをDESで暗号化するのは、 ϕ_1 も ϕ_2 も同一の考え方である。

14 ページ

尚、タイマー時刻については、電源オン時に必ず1回校正し、以降一定の間隔でタイマーを校正するようにしても良い。

発明の効果

以上の如く、本発明により、一定期間経過後、料金不払端末は自動的に暗号化の解読ができなくなり、不正解読は極めて困難で、以下に示す効果も得られるものである。

- (1) タイマーで、料金不払端末の動作を停止。
- (2) タイマーの構成信号は暗号化してあり解読できない。
- (3) 比較的長期間使用の鍵をEEPROMに入れるので、電源がオフになっても、鍵が残る。
- (4) DESによる時刻情報の復号化を1時間に1回としておいても電源オン時1分以内に、タイマーが校正され、かつ、DES復号時間を短かくできる。

4、図面の簡単な説明

第1図は本発明の一実施例における端末制御方式を具現化する端末制御装置のブロック図、第2

15 ページ

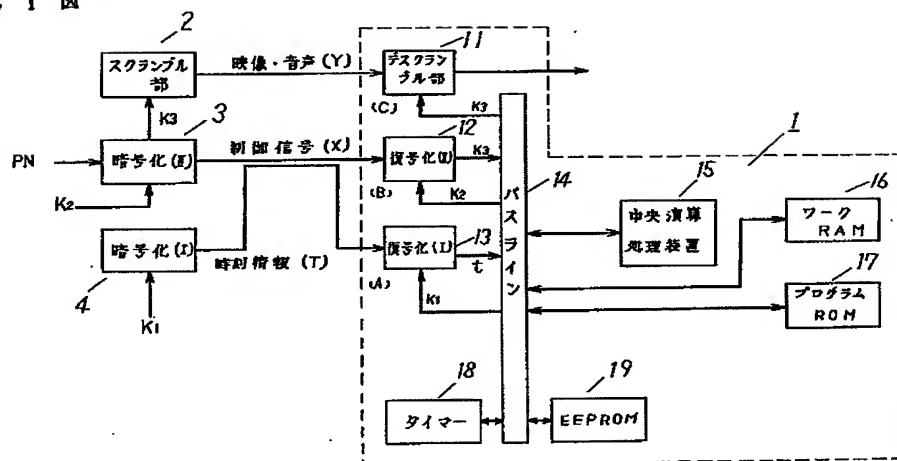
特開昭63-220684 (5)

図は同パケット構成を示す状態図、第3図、第4図は同装置の概略構成を示すブロック図である。

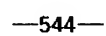
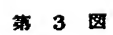
1……信号処理部、2……スクランブル部、3、4……暗号化部、11……デスクランブル部、12、13……復号化部、14……バスライン、15……中央演算処理装置、16……ワークRAM、17……プログラムROM、18……タイマー、19……EEPROM。

代理人の氏名 弁理士 中 尾 敏 男 ほか1名

第1図



第 2 図



特開昭63-220684 (7)

第 4 図

